EXPRESS5800/A1160

System Planning Guide

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of NEC Corporation of America, Inc. and/or its licensors. NEC Corporation of America and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The NEC Corporation of America product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by NEC Corporation of America.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC Corporation of America is prohibited.

Trademarks

Windows is a registered trademark of Microsoft Corporation.

Intel and Itanium are registered trademarks of Intel Corporation.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

PN: 456-01804-001 **August, 2009**

Copyright 2009
NEC Corporation of America
10850 Gold Center Drive, Suite 200,
Rancho Cordova, CA 95670
All Rights Reserved

Contents

Section 1 Introduction 1-1

1.1. Customer-Provided Hardware 1-1

1.2. New Sources of Documentation 1-2

1.2.1. Product Support Web Site 1-2

Section 2 Understanding the System Environment 2-1

2.1. System Components 2-1

2.2. Network Components 2-2

Section 3 Physical Specifications 3-1

3.1. Cabinet Specifications 3-1

3.2. Cell Specifications 3-1

Section 4 Electrical Specifications 4-1

4.1. AC Entrance Specifications (200 to 240 V) 4-1

4.2. Grounding Requirements 4-2

4.3. Signal Reference Connection Requirements 4-2

4.4. Uninterruptible Power Supply 4-2

Section 5 Environmental Specifications 5-1

5.1. Environmental Requirements 5-1

5.2. Shock and Vibration 5-1

5.3. Air-Conditioning Load 5-2

5.4. Noise Specifications 5-2

5.5. Electromagnetic Field Emissions Specifications 5-2

Section 6 Site Considerations 6-1

6.1. Equipment Access 6-1

6.2. System Considerations 6-1

6.3. Service Access 6-2

6.4. Installation in Customer-Provided Cabinets 6-2

6.5. Power Cabling 6-2

6.5.1. Power Cabling for 200V to 240V Systems 6-2

Section 7 Site and Installation Readiness 7-1

7.1. Power 7-1

7.2. Cabinet Acclimatization 7-1

Section 8 Network Planning 8-1

8.1. System Network Traffic 8-1

8.2. LAN Configurations 8-1

8.3. LAN Ports 8-1

8.4. Typical LAN Configuration 8-2

8.5. Operations LAN Configuration 8-4

8.6. Implementing Your Desired LAN Configuration 8-5

8.7. Managing Multiple Enterprise Servers 8-5

8.8. Selecting a Method for Communication with the Support Center 8-5

8.9. Microsoft Active Directory 8-6

8.10. Microsoft Terminal Services 8-6

8.11. Default MLAN IP Addresses 8-7

8.12. Configuring Corporate Firewalls to Communicate Support Information 8-8

8.12.1. Prerequisites to Use the Internet for Transmissions 8-8

Section 9 Security Planning 9-1

9.1. Security Notice 9-1

9.2. LAN Configurations 9-2

9.3. Security Protection Measures 9-2

Appendix A PCI Bus A-1

A.1 PCI Bus Numbering A-1

Appendix B Services and Responsibilities B-1

B.1 Warranty and Services Overview B-1

B.2 Installation and Support Responsibilities B-2

Figures

Figure 6-1 Power-Strip Power Cord Routing..... 6-3
Figure A-1 PCI Slot Numbering A-1

Tables

Table 4-1 Available Power Cords and Mating Receptacle Requirements.....4-1
Table 5-1 Normal Environmental Requirements 5-1
Table 5-2 Normal Environmental Requirements When Shipped or Stored.....5-1
Table 5-3 System Heat Dissipation.....5-2
Table 6-1 Cabinet Service Access Recommendations 6-2
Table 7-1 Cabinet Acclimatization 7-1

Using This Guide

This guide contains information that helps you prepare your site for the installation of an Express5800/A1160 server. By following these site preparation guidelines, you can help ensure a smooth and successful installation of your server. This guide is intended for system administrators and facilities personnel who are preparing the site for installation of an Express5800/A1160 Server.

Proper site preparation and maintenance are vital to the reliability of any computer system. As our customer, it is your responsibility to ensure that the proper facility resources and conditions are maintained. This will allow us to provide support services in accordance with the *NECCare™ Maintenance and Service Warranty Program*.

This guide includes:

- A site planning overview
- Facility requirements
- Electrical requirements
- Environmental requirements.

Who Should Use This Guide

This guide is intended for system administrators and facilities personnel who are preparing the site for an Express5800/A1160 server installation.

Symbols and Conventions

This guide uses the following text conventions and graphic symbols.

Warnings, cautions, and notes have the following meanings:

⚠WARNING

Warnings alert you to situations that could result in serious personal injury or loss of life.

⚠CAUTION

Cautions indicate situations that can damage the system hardware or software.

Note: Notes give important information about the material being described.

- Names of keyboard keys are printed as they appear on the keyboard. For example, **Ctrl**, **Alt**, or **Enter**.
- Text or keystrokes that you enter appear as boldface type. For example, type **abc123** and press **ENTER**.
- File names are printed in uppercase letters. For example, AUTOEXEC.BAT.

Related Documents

In addition to this guide, the following system documentation is useful.

- *NECCare™ Guide*
  The NECCare Guide contains information about NEC's warranty and server registration.

Safety Notices

⚠WARNING

To avoid a risk of injuries, maintenance procedures require trained technical personnel.

In maintenance procedures with voltages of 42.4V peak or 60Vdc or more, take safety measures, such as wearing insulated rubber gloves. Performing work without these measures may cause electric shock.

In an emergency, such as a dangerous event that requires turning off the power supply, turn off the breaker at the rear of the server. Turning off the breaker may cause data destruction. Therefore, users should determine when to turn off the breaker in accordance with specified operation criteria.

The server is equipped with a front stabilizer. Engage the front stabilizer during installation. For stability and to distribute the weight, also attach side stabilizers. Otherwise, the rack may topple over and cause injuries.

If you extend two or more devices from the rack at the same time, the rack may topple over on you. Extend only one device from the rack at a time.

Exercise great care not to hurt your fingers on the rail when you mount/dismount the equipment into/from the rack.

Lithium batteries can be dangerous. Improper handling of lithium batteries may result in an explosion. Dispose of lithium batteries as required by local ordinance. Replace only with the same or equivalent type battery.

A liquid crystal display is used in this server. When handling a damaged liquid crystal display, take care to avoid exposure to the liquid inside the liquid crystal display. The liquid can cause bodily harm. In the event the liquid is ingested, gargle at once and consult a doctor immediately. If the liquid comes in contact with skin or gets into the eyes, wash the skin with cool running water, or flush the eye with cool running water for at least 15 minutes and consult a doctor.

The DVD-ROM drive uses a laser beam. Do not look or insert a mirror inside while the system is on. A laser beam is invisible; if your eyes get exposed to it, there is a risk of losing your eyesight.

- Elevated Operating Ambient Temperature – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient environment. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum rated ambient

temperature of 89.6°F.

- Reduced air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- To prevent fires, and damage to rack equipment and supply wiring, make sure that the rated load of the power branch circuit is not exceeded. Equipment nameplate ratings should be used when addressing this concern. For more information on installation and wiring of power-related facilities, contact your electrician or local power company.
- To prevent electrical shock, connect all rack and rack support equipment to the same electrical circuit of the building wiring. If you are unsure, check the building wiring to avoid remote earth conditions.
- For safe operation, only connect the equipment to a building supply that is in accordance with current wiring regulations in your country. In the USA those wiring standards are regulated by Underwriter Laboratories (UL); in the U.K. by the Institution of Electrical Engineers, (IEE) and in Canada by the Canadian Standards Association (CSA).

⚠WARNING

Some locations within the server have high voltage and therefore are very dangerous. To avoid risk of electric shock, turn off all server power and disconnect power cables before working inside the server unit.

The main power of your server is turned off by turning off the power source to the server or removing the power cable.

Before touching the parts in the server, wait for at least 10 to 15 seconds until residual voltage is discharged.

- Online maintenance – During and after servicing, do not leave the server door open unless necessary to perform servicing.

⚠WARNING

Take care not to short live components with conductive tools, such as an adjustable wrench.

To prevent shock, take care not to drop or leave conductive parts, such as a screw, in the server when servicing the system.

Be careful when accessing a fan or rotating parts to avoid cutting your hand or fingers.

- Safety inspections – When servicing the system, check equipment that can cause harm due to deterioration, and if necessary, replace the part.

Safety Notices for Users Outside of the U.S.A. and Canada

- PELV (Protected Extra-Low Voltage) Integrity: To ensure the extra-low voltage integrity of the equipment, connect only equipment with mains-protected electrically-compatible circuits to the external ports.
- Remote Earths: To prevent electrical shock, connect all local (individual office) computers and computer support equipment to the same electrical circuit of the building wiring. If you are unsure, check the building wiring to avoid remote earth conditions.
- Earth Bonding: For safe operation, only connect the equipment to a building supply that is in accordance with current wiring regulations in your country. In the USA those wiring standards are regulated by Underwriter Laboratories (UL); in the U.K., by the Institution of Electrical Engineers, (IEE) and in Canada by the Canadian Standards Association (CSA).

Section 1

Introduction

System planning is a course of action intended to influence and determine decisions, actions, and other matters as they relate to integrating the system into your environment.

This guide provides the information you need to plan your system and networking environment.

Audience

This guide is intended for the personnel responsible for planning and configuring the system and networking environment.

Documentation Updates

This document contains all the information that was available at the time of publication. The latest version of the document may be found in the Product Support Web Site:

http://support.necam.com/servers/Enterprise/

1.1. Customer-Provided Hardware

The following customer-provided hardware is required to complete the installation:

- LAN cable for the maintenance LAN
  - CAT5 cable
- Additional LAN cables (CAT5 or CAT6 - Gigabit) for connection to the public LAN
- Keyboard, video, and mouse for each partition
  - USB keyboard and mouse for each partition
  - Monitor for the partition

    The keyboard, video display, and mouse (KVM) must be directly connected to the component during installation and cannot be redirected to a remote workstation. After installation is complete, the keyboard, video display, and mouse need not remain connected and can be removed. Multiple keyboard, video, and mouse connections can be provided by the use of a KVM switch in larger system configurations.

- Dedicated Ethernet hub, router, or gateway depending on the LAN topology at your site

1.2. New Sources of Documentation

The following topics describe sources of documentation for your system.

1.2.1. Product Support Web Site

All technical documentation is now available from the Product Support Web Site:

http://support.necam.com/servers/Enterprise/

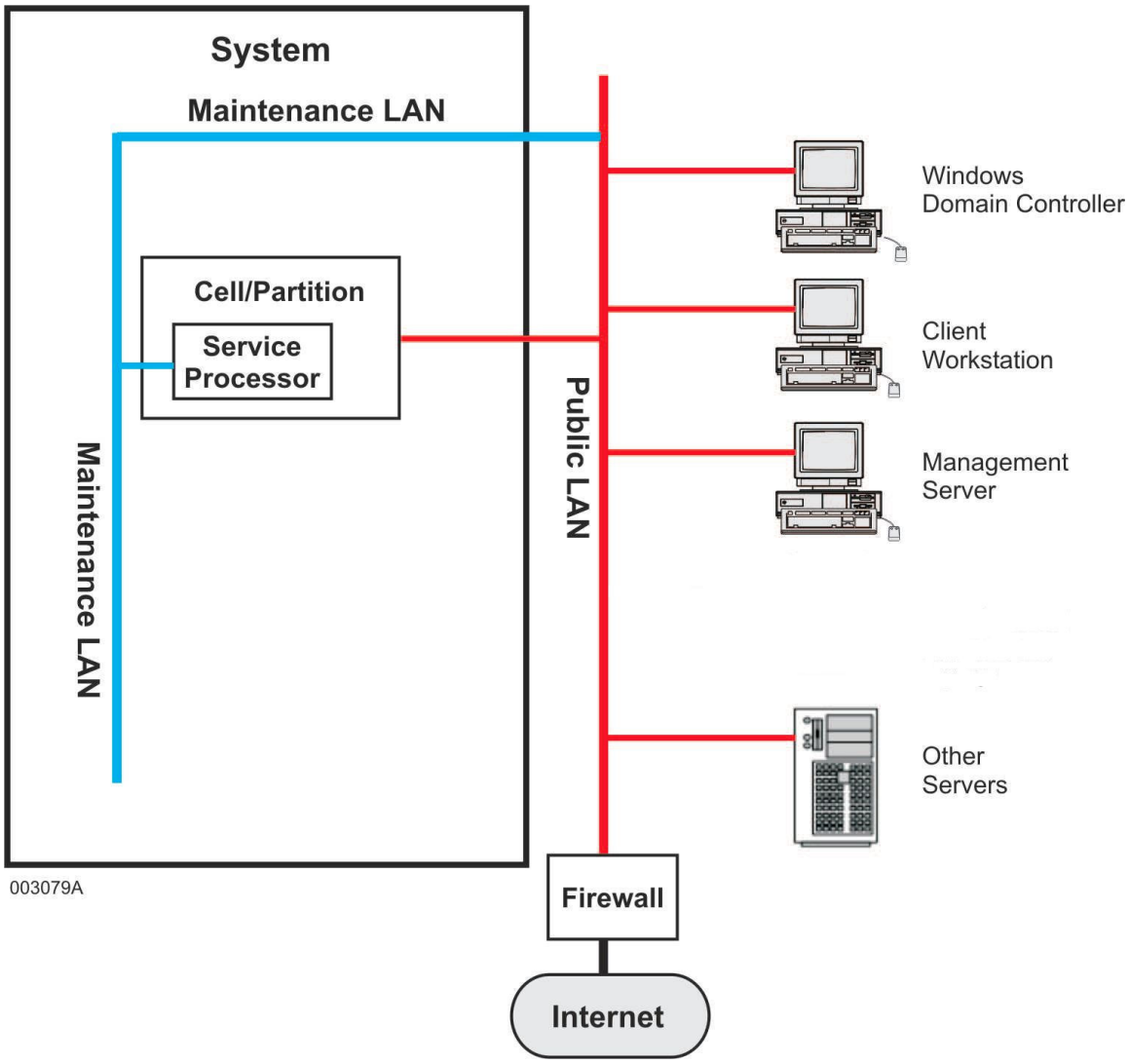
Section 2

Understanding the System Environment

To understand the system environment, you need to become familiar with the system and network components.

2.1. System Components

The following illustration shows how the components are connected in a typical system environment.



Your system can include the following components.

Cells

A cell contains the physical resources of the system: instruction processors, memory, input/output devices, peripheral storage devices, management board, fans, power supplies, control panel, and so on. Each system comprises one to four cells.

Maintenance LAN (MLAN)

The maintenance LAN (MLAN) connects the internal components of the system.

Partition

A partition is a combination of one to four cells that runs a single instance of an operating system or virtual machine monitor. The operating system can be Red Hat Linux, or any supported Windows operating system. The virtual machine monitor can be VMware ESX or Xen. You can purchase the operating system or virtual machine monitor from NEC or supply it yourself.

A system comprises a minimum of one and a maximum of four partitions.

Service Processor

Each cell has an internal management board. For each partition, one of the partition's management boards serves as the Service Processor. (Other management boards in the partition are called satellite management controllers.) A Service Processor manages and maintains the partition, monitors the system for hardware problems, and allows you to repartition the system.

The system's management firmware resides on flash memory on the management board and provides the Service Processor functionality. Using a Web browser, you connect to the management firmware Web interface to maintain, monitor, and repartition the system. The management board also includes the BIOS and Remote Console firmware.

2.2. Network Components

Your network environment can include the following components.

Public LAN

The public LAN is the customer's internal production network that connects the servers, workstations, and so forth of an enterprise. It is sometimes referred to as the enterprise LAN.

Windows Domain Controller

The domain controller typically acts as the Domain Name System (DNS), Windows Internet Name Service (WINS), and Dynamic Host Configuration Protocol (DHCP) server.

Note: *DNS and WINS servers must be made secure in accordance with local security policy guidelines. Microsoft recommends that production applications such as Server Management software not be installed on domain controllers. For more information about domain controllers, see the appropriate Microsoft documentation.*

Management Server

A management server that has Server Management software installed enables you to manage new Express5800 systems and monitor older Express5800 systems in your environment. A management server is necessary in order for your system to report problems to the NEC client support center using remote maintenance service requests.

The ESMPRO Manager is installed on the management server, and it is the main user interface for the Server Management software. It is designed to help you manage your enterprise at a glance.

Client Workstation

A client workstation enables you to remotely access management server functionality. From a Web browser on the client workstation, you can also access the Remote Console interface residing on the partition Service Processor. In addition, a client workstation can serve as a remote system console by accessing the KVMS Redirection page of the Partition Remote Console interface.

Section 3

Physical Specifications

The following topics contain the physical specifications for the cabinet and components. If additional detail is required, contact your NEC service representative.

3.1. Cabinet Specifications

The following topic describes the cabinet specifications.

Dimensions	External Cabinet	Cabinet Rack	Boxed for Shipment
Height	201.93 cm (79.5 in.)	186.7 cm (73.5 in.)	210.82 cm (83 in.)
Width	60.68 cm (23.89 in.)	48.26 cm (19 in.)	89.23 cm (35.13 in.)
Depth	117.22 cm (46.15 in.)	71.76 cm (28.25 in.)	128.27 cm (50.5 in.)

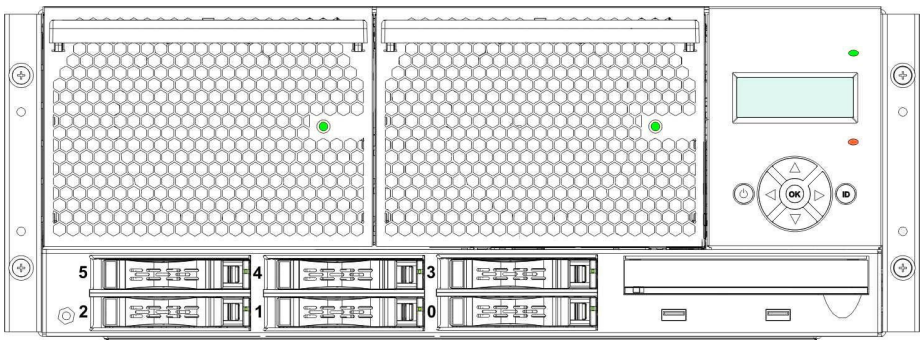
Cabinet Configuration	Weight
Empty cabinet	171.46 kg (378 lb)
One-cell system	216.82 kg (478 lb)
Four-cell system	352.90 kg (778 lb)

Optional Cabinets

Cabinets from other suppliers can also be used if desired. System rack-mounted components can be installed in any cabinets that conform to the Electronic Industries Association specification EIA-310, Racks, Panels and Associated Equipment.

3.2. Cell Specifications

The following topic describes the cell specifications.



Frequency	Voltage	Amperes	Power Consumption	Dual AC Input
50/60 Hz	200 - 240 V	7.5 A at 200V	1450 W - 4948 BTU/hr	Yes

Dimensions		Weight
Width	48.26 cm (19 in.)	47.63 kg (105 lb)
Depth	71.12 cm (28 in.)	
Height	17.78 cm (7 in.)	

Section 4

Electrical Specifications

Major system components, such as the processor/memory cell, are independently powered. Power strips are used to consolidate power cords to reduce the number of branch circuits required.

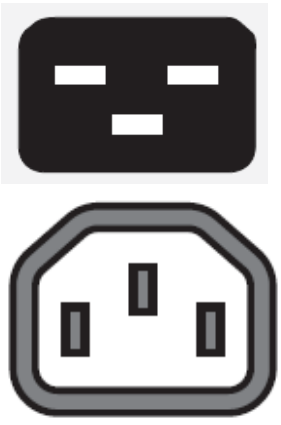
4.1. AC Entrance Specifications (200 to 240 V)

NEC provides two power cords per cell. You must select the appropriate power strip, power distribution unit – PDU or uninterruptable power supply - UPS based on your location and provide the applicable mating receptacle.

The AC entrance requirements, available power cords, and mating receptacle requirements are listed in the following tables.

Receptacles should be positioned as close as possible to the cable access opening at the rear of the cabinet to avoid placing undue stress on the power cords.

Table 4-1 Available Power Cords and Mating Receptacle Requirements

Locality	Power Cord Type	Mating Receptacle (Customer-Supplied)
USA and Canada	C19 – C14 	C13

4.2. Grounding Requirements

Cells in the system have high leakage current and require special handling of the equipment-grounding (earthing) conductor. The safety ground is provided in the power cord. There are no special grounding requirements unless the LC1–UVH power cord is chosen. If this power cord is chosen, the safety ground must be handled as follows:

- The equipment-grounding conductor must be identical in size and in the material thickness to the insulation to the LC1–UVH power cord.
- The equipment-grounding conductor must be green and can have one or more yellow stripes.
- The equipment-grounding conductor must be connected to the grounded circuit conductor (neutral), to the grounding electrode conductor, or to both at the service equipment or at the source of a separately derived system.

4.3. Signal Reference Connection Requirements

If a signal reference grid already exists at the installation site, connect all cabinet braided ground straps to it. The cabinet has a braided ground strap at the bottom of the frame in the rear of the cabinet. Bolt the free end of the strap to the signal reference grid.

Connect any peripheral cabinets to the same signal reference grid. The peripheral cabinets might not have a signal reference connection point. Find a paint-free area near the bottom of the cabinet, and connect the cabinet to the signal reference grid using a signal reference strap. Once the connection is made, use an ohmmeter to verify that the electrical connection is less than 1 ohm.

4.4. Uninterruptible Power Supply

The uninterruptible power supply (UPS) can be used at sites where system downtime because of AC disturbances must be minimized. The UPS uses batteries to provide AC to its load when various types of AC input disturbances occur. The duration of UPS support time depends upon the relationship between UPS capacity and output loading.

The decision to provide alternate power sources, standby power generation, UPS, or a combination of these should be based on the economic consequences of system interruption because of power outages or brownouts (low voltages). The NEC Direct representative can assist in this area.

Section 5

Environmental Specifications

The following topics contain the environmental and climatic requirements for the site.

5.1. Environmental Requirements

Table 5-1 lists the environmental requirements for normal operation of the server. A dedicated computer room or a raised floor environment is optional.

Table 5-1 Normal Environmental Requirements

Environmental Measure	Limits
Temperature	13° C to 35° C (55° F to 95° F)
Relative humidity	10 to 80 percent (non-condensing)
Altitude	–15.2 m (-50 ft) to 2436 m (8,000 ft)

Note: *A cell automatically powers down if the inlet temperature exceeds 40° to 42° C (104° to 107.6° F).*

Table 5-2 lists the environmental requirements for the system when it is shipped or stored.

Table 5-2 Normal Environmental Requirements When Shipped or Stored

Environmental Measure	Limits
Temperature	–40° C to 65° C (–40° F to 149° F)
Relative humidity	95 percent maximum (non-condensing)
Altitude	Sea level to 4.25 km (14,000 ft)

5.2. Shock and Vibration

Avoid installing the system in areas where excessive shock or vibration might occur. Excessive vibration can loosen cables, printed circuit assemblies, and component connections, or cause mechanical failure.

5.3. Air-Conditioning Load

Fans in system components provide sufficient airflow for thermal management within the standard cabinet. The airflow is exhausted at the rear of the cabinet.

Your air-conditioning capacity needs to support the additional heat dissipation for your system. The figures shown in the following table are for a typical cabinet configuration.

Table 5-3 System Heat Dissipation

System	Worst-Case Heat Dissipation
Minimum system (one cell)	1.16 kW (3974 Btu/h)
Maximum system (four cells)	10.15 kW (34656 Btu/h)

5.4. Noise Specifications

The following configurations have been tested according to ISO 7779 and meet the open-office environment standard for noise (NEC standard 4000 0093):

- 1 cell – 59.6 dB*
- 2 cells – 63 dB (estimated)*
- 4 cells – 66 dB (estimated)*

* Below 22° C (71.6° F) ambient temperature

5.5. Electromagnetic Field Emissions Specifications

All system configurations are designed to meet electromagnetic field emission limits as defined in NEC standard 4000 0069. Available system configurations have been tested and meet that standard and the U.S., European, and International electromagnetic field emission requirements for ITE products as described in the following documents:

- U.S. - 47 CFR Part 15, Sub Part B
- European - EMC Directive
- International - CISPR 22, Class A

Section 6

Site Considerations

The site must comply with local and national building, electrical, and safety codes and with all requirements of authorities that exercise jurisdiction in the area of the installation site. The site must also comply with all current applicable standards of the National Fire Protection Association (NFPA) or equivalent local authority.

6.1. Equipment Access

The ease of access to the installation site has a considerable effect on delivery time and expense. Both access for the equipment and access for the installation personnel should be considered. The following factors should be considered when choosing a location, and especially when planning new construction:

- Doors - number and size

  Single doors must be at least 91.4 cm (36 in.) wide and 213 cm (84 in.) high. Double doors 213 cm (84 in.) high that open to 213 cm (84 in.) wide are preferred. When assessing access clearances, remember that cabinets boxed for shipment are 210.82 cm (83 in.) high.

- Hallways - size and number of turns

  Hallways must be at least 152 cm (60 in.) wide and 213 cm (84 in.) high.

- Elevators - size, weight limitations, and hours available
  - Elevators must have a load rating of at least 907 kg (2,000 lb.).
  - Elevator dimensions must be at least 213 cm (84 in.) high, 183 cm (72 in.) wide, and 183 cm (72 in.) long.
  - The elevator door must open to at least 91.4 cm (36 in.) wide by 213 cm (84 in.) high.
- Floors - type of covering and load-bearing capacity
- Ramps - location and slope
- Loading dock - hours available, height, and distance to the computer area

6.2. System Considerations

The system consists of cell-based, rack-mounted servers installed in cabinets in one-partition to four-partition configurations. A minimum system contains a single partition consisting of one cell.

Your system configuration can include other components.

Systems can be installed in a NEC 42U cabinet, or in a customer-provided cabinet.

6.3. Service Access

NEC recommendations for normal service or maintenance activities are shown in the following table.

Table 6-1 Cabinet Service Access Recommendations

Cabinet Access	Minimum Clearance
Front	96.52 cm (38 in.)
Rear	96.52 cm (38 in.)
Side	None

6.4. Installation in Customer-Provided Cabinets

Systems can be installed in any customer-provided standard 19-inch-wide cabinet that meets EIA-310 standards and the following requirements:

- Rails must accommodate items 60.96 to 81.28 cm (24 to 32 in.) in length.
- Rails must support the system component weight. Most system components include their own rails.
- Doors must open wide enough to provide sufficient clearance for maintenance access. The entire rack width must be accessible.
- Doors must not impede airflow for system cooling. Airflow across the cells must be unrestricted.

6.5. Power Cabling

Power cable routing is shown below.

6.5.1. Power Cabling for 200V to 240V Systems

Refer to Figure 6-1 on power cabling for 200V to 240V systems.

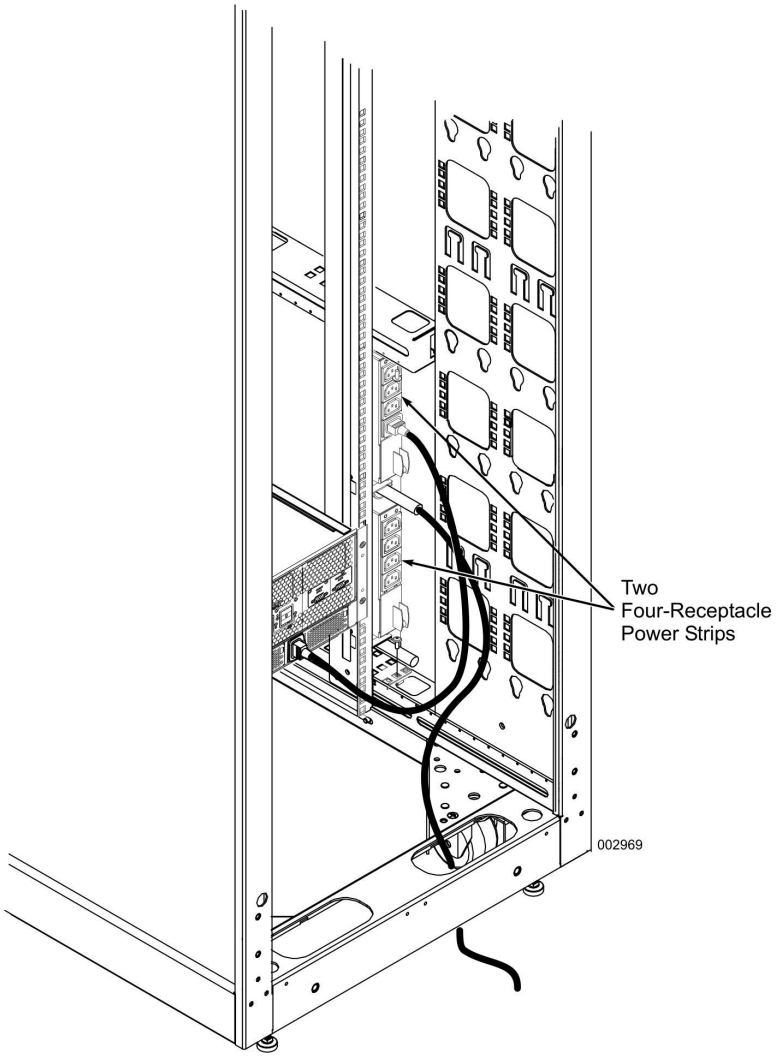


Figure 6-1 Power-Strip Power Cord Routing

Section 7

Site and Installation Readiness

The following topics provide additional information to help ensure the site is ready for installation of the system.

7.1. Power

Site-provided power, cabling, signal reference grid, and UPS should be installed and functioning prior to equipment delivery. If cable troughs for the inter-cabinet signal cables and network communications lines are needed, install the cable troughs prior to equipment delivery. Also, verify that the provided power source is correct.

7.2. Cabinet Acclimatization

The cabinets require an acclimatization period, depending on the ambient shipping temperature. Refer to the following table and ensure that the required time has elapsed before unpacking the cabinets.

Table 7-1 Cabinet Acclimatization

Ambient Shipping Temperature	Acclimatization Period
7.8° to 10° C (46° to 50° F)	1 hour
5° to 7.2° C (41° to 45° F)	2 hours
0° to 4.4° C (32° to 40° F)	3 hours
–5° to –0.5° C (23° to 31° F)	4 hours
–10° to –5.5° C (14° to 22° F)	5 hours
–28.8° to –10.5° C (–20° to 13° F)	6 hours

Section 8

Network Planning

This section describes the system management environment and indicates what you must do to fully use it.

Planning ahead helps ensure that your network enables you to take advantage of the benefits that your system configuration and server management software provide.

8.1. System Network Traffic

Your system requires the following types of information flow across your network environment:

- Server Management software operations traffic

  Server Management software is the centralized operations environment for your system. Communication between the various Server Management software components of your system depends upon your LAN topology.

- Server Management software support traffic

  The Server Management software support traffic, which includes traffic from the Remote Maintenance components, communicates through the Internet with the NEC Support Center.

8.2. LAN Configurations

Your LAN topology will determine how you integrate the system into your environment. You can integrate the system in a typical LAN environment where all traffic passes through your public LAN. An operations LAN, where operations and enterprise management solution traffic is isolated from your other network traffic, adds additional security. Because LAN topology is so diverse, there can be other considerations that apply to your configuration.

8.3. LAN Ports

The following LAN ports are accessible on the rear panel of each cell:

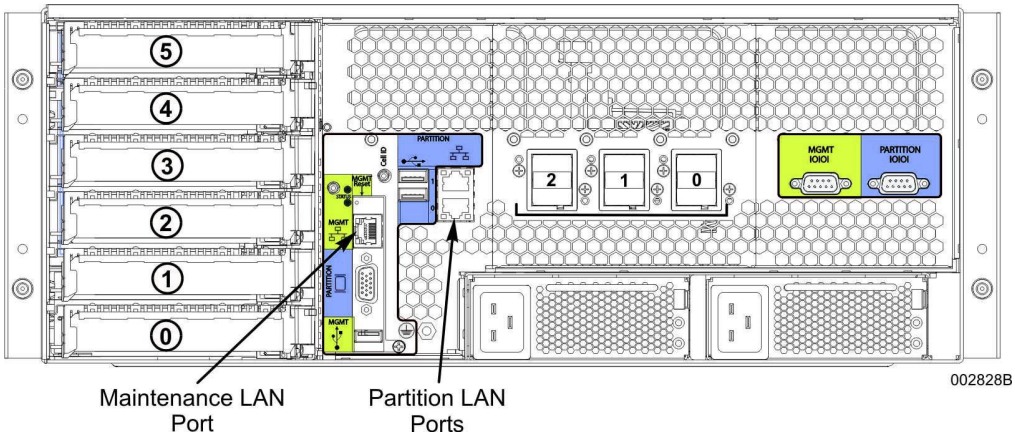
- One maintenance LAN port

  An RJ45 port on the rear of each cell provides a 10/100 Mbps Ethernet network connection to the maintenance LAN.

- Two partition LAN ports

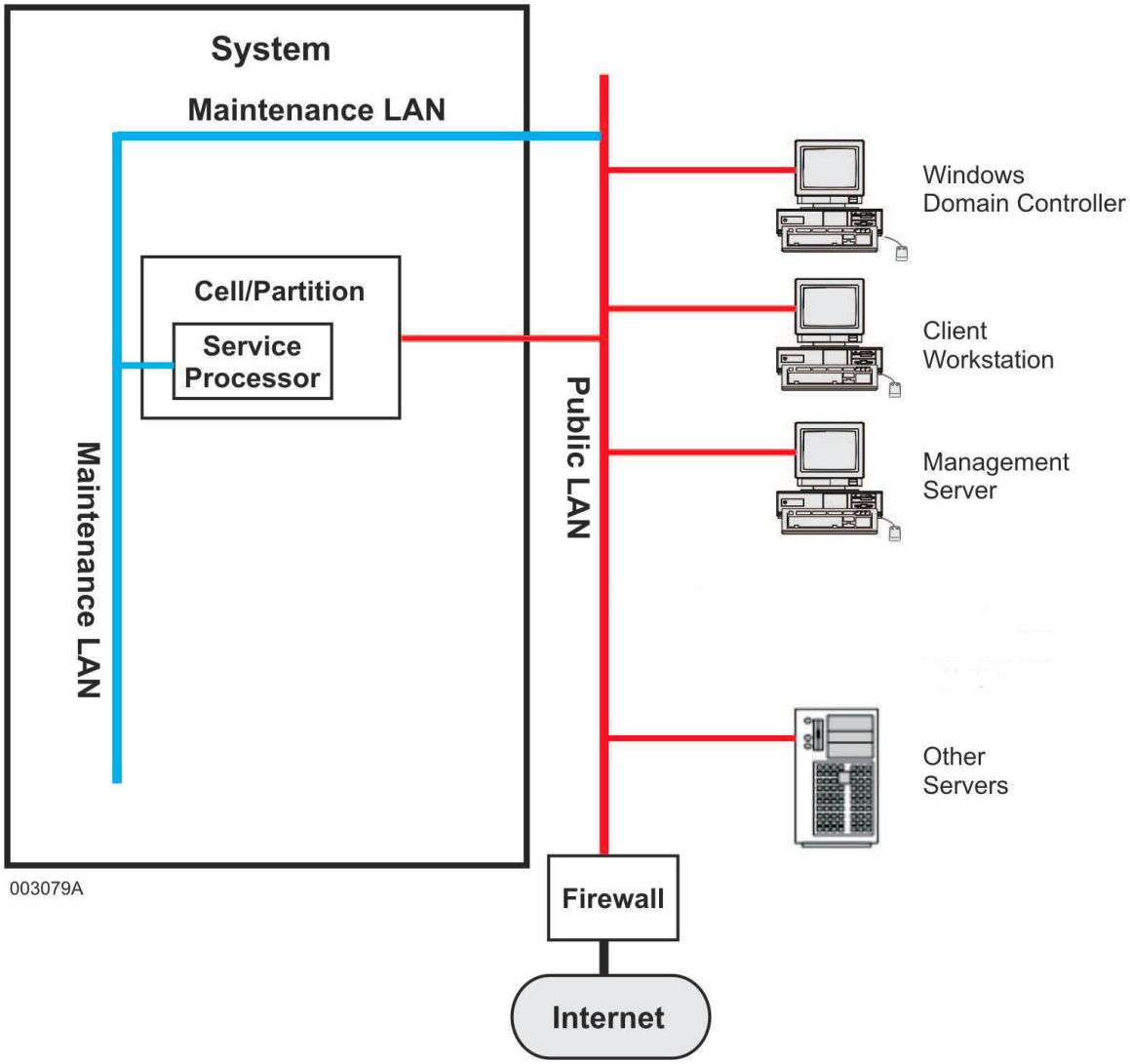
  Two RJ45 ports on the rear of each cell provide 10/100/1000 Mbps Ethernet network connections for the operating system to use. These are normally connected to your public LAN.

The following illustration shows the LAN ports that are accessible on the rear panel of each cell.



8.4. Typical LAN Configuration

The following is a typical LAN configuration for your system.



Advantages

A typical LAN configuration has the following advantages:

- This is a simple LAN topology.
- Additional network components are not required.

Disadvantages

A typical LAN configuration has the following disadvantages:

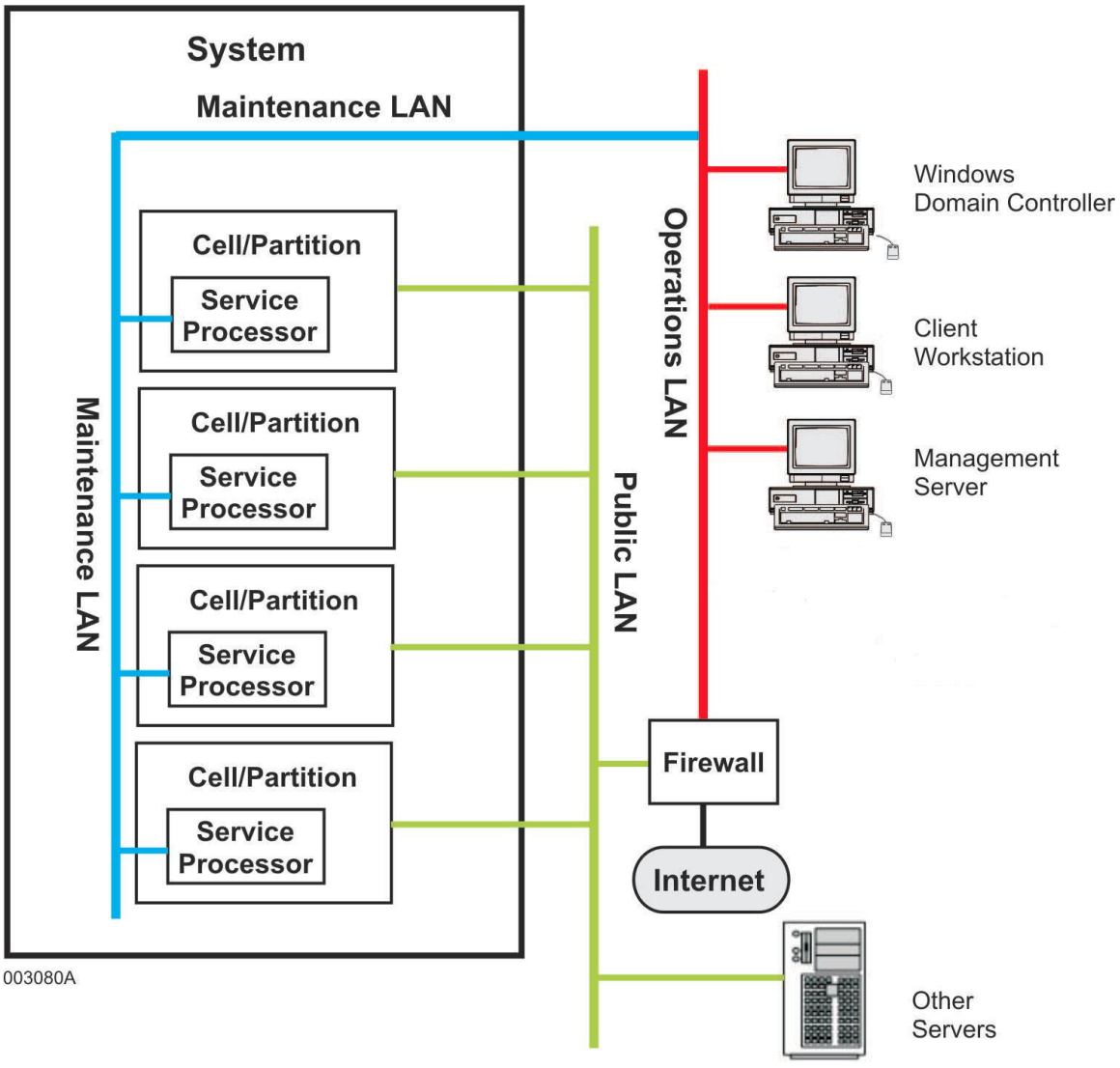
- In this configuration, operations and enterprise management solution traffic pass through your public LAN.
- If you have multiple systems, additional traffic loads are placed on your public LAN.

- Setting up and maintaining strong network security for the maintenance LAN can be a challenge.

8.5. Operations LAN Configuration

The operations LAN is an isolated network which connects the maintenance LAN to management components (such as workstations or management servers) associated with one or more systems.

The following illustration shows the operations LAN.



Operations LAN Advantages

An operations LAN has the following advantages:

- The operations LAN isolates operations and enterprise management solution traffic from your public LAN. This isolation is provided by using a firewall between the operations LAN and public LAN or by not connecting to the public LAN.
- This configuration helps overcome the challenges of setting up and maintaining a secure network. It provides strong network security for the maintenance LAN while offering simple, straightforward access for authorized users.
- This configuration provides remote serviceability without compromising system security.
- If you have multiple systems, you can manage them with a single operations LAN.

Operations LAN Disadvantages

An operations LAN has the following disadvantages:

- Additional network components are required.
- Additional network administration is required.

8.6. Implementing Your Desired LAN Configuration

Once you have decided whether to use a typical LAN configuration or an operations LAN configuration, the *Express5800/A1160 Hardware Installation Guide* will show you how to cable the system. After completing the hardware installation, perform the procedures in the *ESMPRO Manager User's Guide* (on the management server) and then continue with the procedures in the *Software Installation and Configuration Guide* (on the partition). Performing these procedures completes the implementation of your desired LAN configuration.

8.7. Managing Multiple Enterprise Servers

If you have multiple systems, you can manage them with a single management server. Multiple systems can be supported on the same LAN segment with unique IP addresses. These IP addresses are configured during installation and configuration. Problems can occur if the default addresses are used. These default addresses are intended as a means to easily initially bring up a system, and are intended for single system usage only.

8.8. Selecting a Method for Communication with the Support Center

It is recommended that the system be able to communicate support information to the

NEC Support Center. The system can send information through your corporate Internet connection (the preferred method) or a modem.

To obtain optimum performance, an Internet connection is required. Using an Internet connection simplifies communication configuration and management and ensures that all of the Server Management software components function properly. This method is likely to fit better than a modem into your corporate security policy, and when your corporate firewalls are configured correctly, it introduces minimal additional risk. However, if your security policy does not permit your system to communicate through your corporate Internet connection, you can use a modem.

To use the modem, a dedicated telephone line must be installed and maintained in close proximity to the system and you must configure your system to use it.

8.9. Microsoft Active Directory

In a server environment that uses Microsoft Active Directory, you can provide authorization for users based on their user accounts. When users attempt to access the operations LAN, they are required to provide a valid user name and password if the user account that the workstation is currently running under is not sufficient. If they cannot, access is denied. Using Active Directory enables you to easily add or remove user authorizations based on information in the directory service and to share security groups among different servers.

If Active Directory is not available in your server environment-or if you want to further restrict traffic within an environment that has Active Directory- you can authorize traffic based on allowable IP addresses or subnets. This provides the benefit of being able to restrict access to Console Manager from the public LAN; only users attempting to access Console Manager from selected IP addresses or subnets would be permitted to do so.

For detailed information about Active Directory, see the Microsoft corporate Web site or your Windows server documentation.

8.10. Microsoft Terminal Services

Remote Console is the primary user interface to each partition. However, you might consider using Microsoft's Terminal Services as an alternate user interface solution for accessing a Windows environment. You can use Terminal Services to remotely execute applications on a Windows-based server from a wide range of devices over virtually any type of network connection (such as from a workstation on your public LAN). With Terminal Services, you can use all display settings available on the client workstation.

For detailed information about Terminal Services, see the Microsoft corporate Web site or your Windows server documentation.

8.11. Default MLAN IP Addresses

The system automatically assigns initial fixed IP addresses to various components within the system. Addresses that are assigned on the maintenance LAN are initially configured in manufacturing using default IP addresses. You must change these default addresses during system installation.

The following text describes system components and the default IP addresses you are expected to change during installation and configuration to integrate the system into your network environment.

Service Processors

Each partition has a Service Processor that is assigned a default maintenance LAN IP address. The default IP addresses are as follows:

```
172.26.2.0 for the first partition "P0"
172.26.2.1 for the second partition "P1" (if any)
172.26.2.2 for the third partition "P2" (if any)
172.26.2.3 for the fourth partition "P3" (if any)
```

These IP addresses exist only if the partition exists. So for example, if a four–cell system has only one partition, only 172.26.2.0 will be in use. One very important point to understand is that these partition IP addresses aren't physically tied to a particular cell, but remain with the partition, no matter what cells that partition is associated with.

Cells (Resource Manager)

Each cell in the system is assigned an IP address by default. The default IP address is dependent upon the cell's identity within the system as follows:

```
172.26.1.0 for Cell 0
172.26.1.1 for Cell 1 (if any)
172.26.1.2 for Cell 2 (if any)
172.26.1.3 for Cell 3 (if any)
```

Partition

No default maintenance LAN IP address is assigned to the partition itself. However, you must assign one using Setup Assistant. The address you assign must allow the management server to communicate with the partition.

8.12. Configuring Corporate Firewalls to Communicate Support Information

The recommended method for communicating support information to the NEC Support Center is to send information through your corporate Internet connection. To successfully and securely communicate through the Internet, you must configure your corporate firewalls to permit the Server Management software components to communicate with the NEC Support Center. Properly configuring the corporate firewalls minimizes the risk of unwelcome intrusions.

To configure your corporate firewalls optimally, consider taking advantage of the security features that many corporate firewalls provide. For example, many corporate firewalls enable you to configure the endpoint hosts that are able to participate in a dialog as well as the protocols and ports that are used.

Another security feature that many corporate firewalls provide is the ability to open ports at scheduled times. When considering whether to use this feature, you should evaluate the advantages and disadvantages of doing so for each Server Management software component.

8.12.1. Prerequisites to Use the Internet for Transmissions

For Remote Support to access the NEC Product Support Web Site using the Internet, the following ports must be opened:

- Remote support protocol HTTPS:
  - Port 443
  - IP address (143.101.250.58)

  Note: *Ports can be set to outbound only for NEC purposes.*

Section 9

Security Planning

Security planning is somewhat dependent on the system configuration; that is, whether the system uses Microsoft Windows or Linux. In Windows configurations, for example, baseline security is provided through the configuration of a standard set of hardware and software components.

Authentication control is used to restrict access to only authorized personnel. Systems are installed using the Microsoft workgroup model, where user names and group memberships are controlled separately on each component. User authentication between these components (including Service Processors, partitions, management servers, and client workstations) relies on synchronized user names and passwords. Domain security, Active Directory security, or both can be used; however, this implementation requires consideration of the firewall and group membership setup requirements.

All systems are installed using either a default password defined by NEC or a customer-defined default password that is used repeatedly throughout the installation and setup process. NEC strongly recommends that the customer should change all passwords set during the installation process to a new password or set of passwords that is defined in conjunction with the customer's security policies. If this is not done, the passwords used during the installation will be retained and be neither private nor secret, nor will they be unique across multiple system installations.

Note: *NEC establishes and maintains a baseline level of security for all systems, and changes are applied in conjunction with standard system firmware updates. Customer-specific input to these security measures is restricted to the use of site-specific passwords. NEC does not explicitly supply Windows security updates. Releases contain platform software updates (for example, service packs) as appropriate.*

9.1. Security Notice

The server default security settings might be inadequate for your environment. In addition, security vulnerabilities might have been discovered after the system software was released. NEC makes no claim or warranty that your system is secure as delivered. Before you connect the server to a network, review the security requirements of your applications, data, and environment. After evaluating your system, implement an appropriate security policy for each environment. Systems with Web services, such as Microsoft Internet Information Services (IIS), installed might require added security considerations. During initial system setup, the system prompts you when it is time to

install any security hotfixes.

9.2. LAN Configurations

Isolated Operations LAN

This configuration is preferred and is the most secure. NEC strongly recommends the use of a fully isolated operations LAN to assure that there is no possibility of outside access to the maintenance/operations LAN components.

In a fully isolated LAN environment, with updates and temporary connections only being made by devices that are determined to be problem free, there is no need for further security protection measures, such as virus protection, software and security updates, and related product updates.

Operations LAN with Firewall Access to the Public LAN

This configuration is less secure, and is not preferred. For sites with access to other enterprise-based devices, NEC recommends the use of a customer-supplied firewall to restrict access between the devices and the maintenance/operations LAN. The level of security provided by a firewall is extremely dependent upon its configuration.

In a fully isolated operations LAN environment with firewall access to public LAN devices, further security protection measures must be taken, such as virus protection, software and security updates, and related product updates.

Open Access to the Public LAN

This configuration is not recommended. For sites with access to the public LAN, security must be defined, and be provided by the customer. Options include the use of customer-supplied firewalls and routers that can filter and otherwise restrict access to the maintenance LAN. Enterprise connection might be desired to provide greater access to operations data from desktop terminals or other devices. However, customers must be aware of the potential risks of infection resulting from this form of configuration.

For configurations with the maintenance LAN connected to the public LAN without an operations LAN, further security protection measures must be taken, including virus protection, software and security updates, and related product updates.

9.3. Security Protection Measures

In addition to the previously mentioned baseline security, some or all of the following steps should be taken to provide additional protection. The steps you need to consider depend on the implementation chosen for the physical and electrical security of the operational environment components.

- Software and security updates
- Security analyzers
- Antivirus software
- Online security and privacy protection software
- Firewall
- Physical access controls
- In-depth defense

Software and Security Updates

Software providers frequently issue software and security-specific updates, also referred to as hot fixes or patches. The changes range from modest updates (or corrections) to more serious and significant areas of change.

Given the frequency of change - and the fact that the changes are directly made available to customers - NEC neither tests, verifies, nor regulates the distribution and installation of these changes. Therefore, the responsibility for the application of changes must be retained by the customer at the site level.

Note: *Some security fixes could possibly break or restrict a function needed by NEC operational software. Customers are strongly advised to test these corrections before implementing them in any mission-critical application.*

NEC does routinely test distributed service packs and formalized product update levels, but has no policy of testing all interim product updates. A major reason for this policy is that NEC does not wish to delay the customer's use of critical changes and security updates, due to the frequency and volume of these changes.

The manner in which security is configured, programmed, or installed into the system is variable based on customer configuration options. Therefore, customers should establish security procedures that address concerns defined in their own security policies.

NEC recommends that only critical updates be applied. Noncritical updates, driver updates, and Service Packs should only be applied when you are directed to do so by NEC. NEC provides specific guidance with regard to the application of updates in Technical Information Bulletins (TIBs).

Security Analyzers

Security analyzers are used to detect security vulnerabilities within computing systems. A number of products can be used to identify common security configuration and security deficiencies on systems with Microsoft operating systems. For example, Microsoft Baseline Security Analyzer (MBSA) is a free, downloadable security product

that provides a streamlined method of identifying common security issues on Microsoft Windows systems.

Antivirus Software

Customers should choose an antivirus product that is recommended by NEC.

Note: *Antivirus software should be installed throughout the maintenance/operations LAN, management servers, workstations, and other components. It is important to update antivirus definition files on a regular basis to ensure that the software addresses currently identified viruses. Antivirus software cannot be installed on the Service Processors.*

Online Security and Privacy Protection Software

Online security and privacy protection software can be purchased to identify and remove tracking software. Examples include SPYBOT and ADAWARE. If these are used, sites must comply with the provider's licensing guidelines. For example, some of these tools are free for private use, but require paid licenses for commercial use.

The IIS Lockdown Wizard functions by turning off unnecessary features, thereby reducing the attack surface available to attackers. Microsoft formerly had two tools used to control IIS configuration and operation: the IIS Lockdown Tool and URLscan. URLscan has been integrated into the IIS Lockdown Wizard. Microsoft states that for this tool to be effective, sites must install all hot fixes (patches) before and after the Lockdown tool is applied.

Firewall

The term "firewall" refers to a system designed to prevent unauthorized access to entities within a network. Firewalls can be implemented either in the form of software (for example, Microsoft Windows XP Internet Connection Firewall), or hardware, or a combination of the two. Typically, they are used to restrict access beyond or between public and private LAN segments. Most often when people refer to a firewall, they mean a hardware component that resides on a network.

Firewalls can block or filter packets of data, specific applications, or data that is sent by way of specific addresses. Generally there is a need to configure a firewall so that it can be suitable for a specific purpose, and so that it meets the needs of a given security policy.

Physical Access Controls

For maintenance/operations LAN configurations that are not fully isolated, customers are advised to regulate access to the LAN by means of physical access controls.

Physical access control includes such things as limited access to facilities, locked rooms, access restriction using smart cards or other access protection media and devices, such as firewalls. Access to secured resources should be audited and a history of access should be available.

Note: *There is a need to restrict access on an "as needed" basis to limit system vulnerability. While unauthorized access to the maintenance/operations LAN cannot result in unauthorized access to customer data, it can lead to problems that result in system "denial of service."*

In-Depth Defense

Security is best established in the form of layered defenses, where no single form of defense is assumed sufficient. What this means is that the best defense is, in fact, a series of defenses that includes security patch management, ongoing security analysis, antivirus protection, and physical access controls.

In addition, effective security includes a firewall and means of continuous improvement. This means that security involves continuous learning. As products, features, and approaches change, there is a need for each site to adjust to these changes.

10.4. Additional Security Considerations

NEC provides a range of security features within the system. However, due to the range of customer-defined configurations - and the frequency with which Microsoft and other vendors provide security-related changes - there might be a need for customers to take additional steps to meet the needs of their own security policies. NEC recommends an absolute physical level of security for the systems, but NEC also recognizes that customers need flexibility to manage their enterprise in a variety of ways. Enterprise management, including the use of third party products and unique customer configurations, requires additional customer considerations. Therefore, beyond the base level of security provided by NEC, the customer must manage the maintenance of security within the enterprise.

Appendix A

PCI Bus

A.1 PCI Bus Numbering

Six PCI slots are available for customer-supplied controllers. The following illustration shows the PCI slot numbering.

Figure A-1 PCI Slot Numbering

Appendix B
Services and Responsibilities

The following topics provide an overview of the warranty and services and explain installation and support responsibilities.

B.1 Warranty and Services Overview

The NEC service warranty provides hardware support and software media replacement. To ensure proper levels of support, customers should review the service warranty, which provides coverage on a next-business-day basis. Coverage includes only those hardware services that are essential in providing basic reactive support. NEC warrants the software media against defects for 90 days.

NEC offers a range of technical support and maintenance services so that customers can select the appropriate support for their systems.

NEC Corporation of America(NECAM)'s Standard NECCare™ Maintenance and Service Warranty Program offers you the following benefits:

- 3 Years of Standard Warranty coverage
- Toll-free hardware technical support, 5 days a week, 8am-5pm (Local time) in the continental US and Canada.
- Next Business Day On-site Repair Support
  - A Certified Service Technician will be on-site on the Next Business Day for repair support once a service call is deemed necessary following trouble-shooting efforts between the Customer and NECAM
  - Replacement parts will also arrive on the Next Business Day after problem diagnosis. Customer must be able to sign and receive parts as requested by NEC to meet Next Day support.

    Note: *NECAM will use commercially reasonable best efforts to provide Next Business Day On-site service provided calls for support are received by 3:00pm, PST. Service Levels are response time objective and are NOT Guarantees. NECAM is not responsible for service calls missed outside the control of NECAM. If your location is outside of a NECAM authorized service coverage area, the response time may be longer and/or an additional travel charge may be assessed. In some cases, on-site service may not be available. All service response times are contingent upon parts availability.*

For more detail, refer to *NECCare™ Standard Warranty Program* and *Premium Warranty Program* for Express5800/A1160 or contact a NEC sale representative to

obtain additional support services.

From increasing system availability to helping customers ensure that the business-critical IT environment delivers on expectations, NEC provides reliable, consistent support.

B.2 Installation and Support Responsibilities

The following tables explain installation and support responsibilities.

Installation Responsibilities

Service Task	Responsibility	Billable Service
Initial system hardware installation	User	Installation charges apply if a customer wants NEC to install a customer-installable system package.
Initial Server Management installation (includes management server installation and configuration)	User	Optional charge applies if NEC performs the service. Various offerings are recommended and available.
Initial system and operating system configuration	User	Optional charge applies if NEC performs the service. Various offerings are recommended and available.

Hardware Upgrades

Service Task	Responsibility	Billable Service
Hardware upgrade	NEC	Installation service charge is typically part of an upgrade style.
Field Change Notice (FCN) upgrade	NEC	Billable service if scheduled outside service hours.

Software/Firmware Upgrades

Service Task	Responsibility	Billable Service
Platform Firmware	User	Upgrade service may be offered by NEC.
Partition operating system and	User	Upgrade service may be offered

applicable drivers		by NEC.
Server management	User	Upgrade service may be offered by NEC.
Server management (management server)	User	Upgrade service may be offered by NEC.

Hardware Maintenance

There are two types of replaceable units on the Express5800/A1160: customer-replaceable units (CRUs) and field-replaceable units (FRUs).

A FRU is replaced by NEC and a CRU is replaced by the customer. FRUs and CRUs are identified in the Express5800/A1160 *User's Guide*.

NEC has two levels of service plans, one in which the client replaces the CRU, and one in which NEC replaces both CRUs and FRUs.

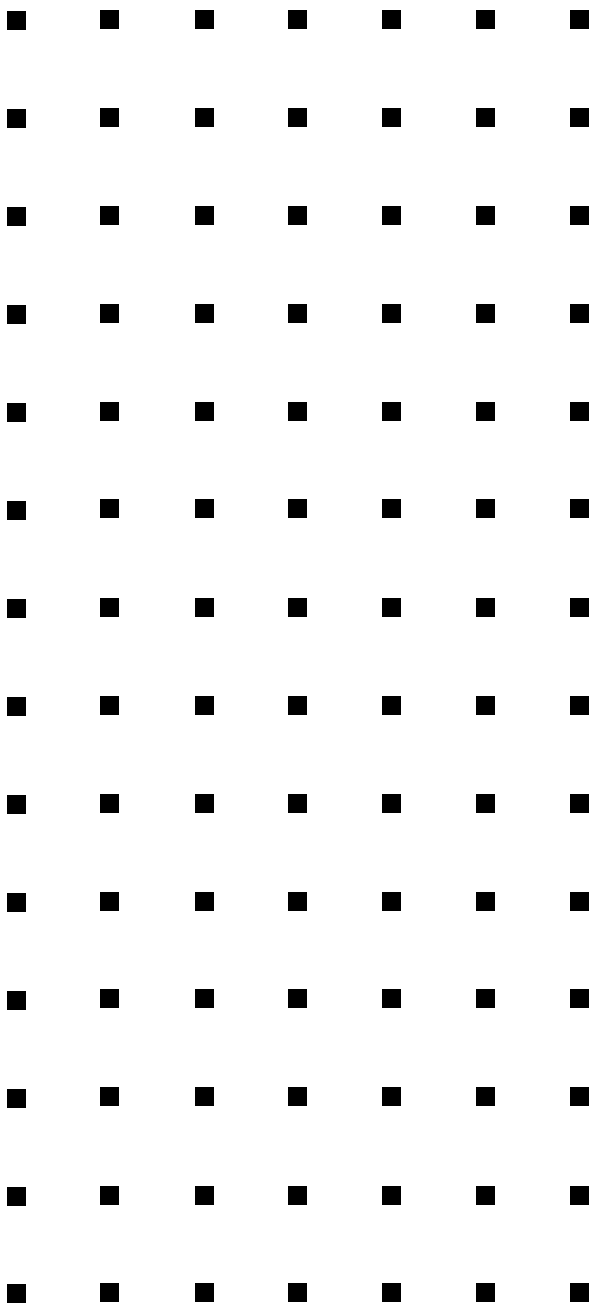
If NEC determines that your issue can be addressed by shipping a replacement part to you for installation in your system (a "Customer Replaceable Unit" or CRU), NEC will ship a replacement part to your site ("replacement CRU"). NEC will use commercially reasonable efforts to send a replacement CRU consistent with the response time set forth in your maintenance agreement.

The client is responsible for ensuring that the malfunctioning part being replaced ("malfunctioning hardware") is returned to NEC in accordance with all NEC shipping or courier instructions. You agree to pay the published list price of any replacement CRU in the event that you fail to return the corresponding malfunctioning hardware. Replacement CRUs will be of new or like-new quality. Replacement CRUs assume the warranty status of the system into which they are installed, or 90 days, whichever is longer.

Note:

Consumers are cautioned that Product performance is affected by system configuration, software, the application, Customer data, and operator control of the system, among other factors. While NEC Corporation of America products is considered to be compatible with many systems, the specific functional implementation by the Customers of the product may vary.

Therefore, the suitability of a product for a specific purpose or application must be determined by the Customer and is not warranted by NEC Corporation of America. For more information, telephone **1-877-NEC(632)-0064**



456-01804-001